Amendments to the Specification:

Please replace paragraph [0074] with the following:

[0074] In preferred arrangements, a trusted third party device 20 includes a processor [[31]] 21 and maintains a register for v in Montgomery representation. The third party device may also be the provider of v and s as the public/private key pair for prover 10, and provide the value of n derived from secret prime numbers p and q.

Please insert the heading, "BACKGROUND" before ¶ [0001];

Please insert the heading, "SUMMARY" between ¶¶ [0005] and [0006];

Please insert the heading, "BRIEF DESCRIPTION OF THE DRAWINGS" between ¶¶ [0026] and [0027]; and

Please insert the heading, "DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS" between ¶¶ [0030] and [0031].

Please insert the following abstract on a separate page (also included in an attached appendix on a separate page):

ABSTRACT

An efficient implementation of zero knowledge protocols for authentication of devices and for identification of devices connecting to a network. According to one aspect, the present invention provides a method of verifying the knowledge of a secret number s in a prover device by a verifier device having no knowledge of the secret number, with a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein.